EXHIBIT C

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

INTRODUCTION

Some voters face challenges voting in-person and by mail. State and local election officials in many states use email, fax, web portals, and/or web-based applications to facilitate voting remotely for groups like military and overseas voters and voters with specific needs.

The Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) assess that the risks vary for electronic ballot delivery, marking, and return. While there are effective risk management controls to enable electronic ballot delivery and marking, we recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place. Recognizing that some election officials are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Notably, we assess that electronic delivery of ballots to voters for return by mail is less vulnerable to systemic disruption.

In this document, we identify risks and considerations for election administrators seeking to use electronic ballot delivery, electronic ballot marking, and/or electronic return of marked ballots. The cybersecurity characteristics of these remote voting solutions are further explored in NISTIR 7551: A Threat Analysis on UOCAVA Voting Systems.

RISK OVERVIEW

	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Technology Overview	Digital copy of blank ballot provided to voter	Making voter selections on digital ballot through the electronic interface	Electronic transmission of voted ballot
Risk Assessment	Low	Moderate	High
Identified Risks	Electronic ballot delivery faces security risks to the integrity and availability of a single voter's unmarked ballot	Electronic ballot marking faces security risks to the integrity and availability of a single voter's ballot	Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and, can occur at scale

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

All states use **electronic ballot delivery** to transmit a digital copy of an unmarked ballot to the intended voter to mark, in compliance with the Military and Overseas Voters Empowerment Act (MOVE). These ballot delivery systems are exposed to typical information security risks of internet-connected systems. The most severe risks to electronic ballot delivery systems are those that would impact the integrity and/or availability of the ballots, such as altering or removing ballot choices. These risks can be reduced and managed through use of appropriate security controls. Additionally, some electronic ballot delivery systems perform functions to verify a voter's identity before presenting them their assigned ballot. The identification process can use personal identifying information, such as name and driver's license number, or biometrics. When this verification is improperly configured, remote electronic ballot delivery systems can present additional privacy risks—like the loss or theft of the voter's personal and/or biometric identity information. These risks may be managed through configuration management and appropriate security controls.

Electronic ballot marking allows voters to mark their ballots outside of a voting center or polling place. Typically, this describes the electronic marking of a digital copy of the blank ballot using the electronic interface. The marked ballot is then returned to the appropriate official. Risks to electronic ballot marking are best managed through the production of an auditable record, meaning the voted ballot is printed and verified by the voter before being routed to the appropriate official. This auditable record is an important compensating control for detecting a compromise of security in remote voting.

Electronic ballot return, the digital return of a voted ballot by the voter, creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk.

Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time. As the National Academies of Science, Engineering, and Medicine write in Securing the Vote: Protecting American Democracy (2018), "We do not, at present, have the technology to offer a secure method to support internet voting. It is certainly possible that individuals will be able to vote via the internet in the future, but technical concerns preclude the possibility of doing so securely at present." If election officials choose or are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Further, election officials should have a mechanism for voters to check the status of their ballot, as required for provisional ballots and military and overseas voters by the Help America Vote Act and the MOVE Act, respectively.

RISK COMPARISON – ELECTRONIC AND MAILED BALLOT RETURN

Some risks of electronic ballot return have a physical analogue to the return mailing of ballots. However, electronic systems present far greater risk to impact a significant number of ballots in seconds.

- **Scale –** While mailing of ballots could be vulnerable to localized exploitation, electronic return of ballots could be manipulated at scale. For mailed ballots, an adversary could theoretically gain physical access to a mailed ballot, change the contents, and reinsert it into the mail. This physical man-in-the-middle (MITM) attack is limited to low-volume attacks and mitigated by proper chain of custody procedures by election officials. In comparison, an electronic MITM attack could be conducted from anywhere in world, at high volumes, and could compromise ballot confidentiality, ballot integrity, and/or stop ballot availability.
- **Bring Your Own Device –** Unlike traditional voting systems, electronic ballot delivery and return systems require a voter to use their own personal devices such as a cell phone, computer, or tablet to access the ballot. A voter's personal device may not have the necessary safeguards in place. As a result, votes cast through "bring your own device" voting systems may appear intact upon submission despite tampering as a result of an attack on the personal device rather than on the ballot submission application itself. Voters using personal devices increase the potential for an electronic ballot delivery and return system to be exposed to security threats.
- **Voter Privacy –** Electronic ballot return brings significant risk to voter privacy. Unlike traditional vote by mail where there is separation between the voter's information and their ballot, many remote voting systems link the two processes together digitally. This makes it difficult to implement strong controls that preserve the privacy of the voter while keeping the system accessible.

TECHNICAL CONSIDERATIONS FOR ELECTRONIC BALLOT RETURN

Some voters, due to specific needs or remote locations, may not be able to print, sign, and mail in a ballot without significant difficulty. While we assess electronic ballot return to be high risk, some jurisdictions already use electronic ballot return systems, and others may decide to assume the risk.

While risk management activities should lower risk, election officials, network defenders, and the public may all have different perspectives on what level of risk is acceptable for the systems used to administer an election. For those jurisdictions that have accepted the high risk of electronic ballot return, the following guidance identifies cybersecurity best practices for internet- and network-connected election infrastructure. The information provided should be considered a starting point and is not a comprehensive list of defensive cybersecurity actions. Even with these technical security considerations, electronic ballot return remains a high-risk activity. Refer to applicable standards, best practices, and guidance on secure system development, acquisition, and usage.

GENERAL

- All election systems and technology should be completely separated from systems that are not required for the implementation or use of that specific system.
- Any ballots received electronically should be printed or remade as a paper record.
- Election officials should implement processes to separate the ballot from the voter's information in a manner that maintains the secrecy of the ballot.

- If the system attempts to verify the voter's identity through digital signature, biometric capture, or other method, assess whether an attacker could use this to violate ballot secrecy.
- The auditability of the results should not rely solely on the data stored digitally within the system.
- Best practices for securing voter registration data should be used to protect the personal identifying information that is stored in the voter registration database and used to authenticate voters.
- Removable storage media (e.g., USB drives, compact flash cards) used to handle sensitive election data should be obtained from a trusted source and erased before being used. To the extent practical, removable storage media should be new.
- Follow the domain security best practices issued by the Federal Government available at https://home.dotgov.gov/management/security-best-practices/

FAX

Facsimile (fax) machines are often used by local election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers should be aware of the risks and challenges associated with fax. Fax has no security protections unless sent over a secured phone line and is generally not considered suitable for sensitive communications. Faxes may be viewed or intercepted by malicious actors with access to phone lines. Furthermore, multipurpose fax machines with networked communications capability can be leveraged by cyber actors to compromise other machines on the network. We recommend election officials using fax machines implement the following best practices.

- Use a no-frills fax machine; multipurpose fax machines typically have modems for external network communications. If you only have a multipurpose fax machine, turn off the Wi-Fi capability and do not plug it into the network—only connect it to the phone line.
- Check the configuration to make sure that the fax cannot print more pages than anticipated from a single fax or ballot package.
- Use a dedicated fax machine and fax line for the distribution and receipt of ballots. Do not make the phone number publicly available, and only provide it in the electronic ballot package for voters who have been authorized to vote using electronic return.
- Election officials should set up transmission reports when faxing a ballot package to the voter to verify that the ballot package was received by the fax machine it was sent to.
- Use a trusted fax machine that has been under your control. Ensure you have enough fax machines and phone lines to handle the anticipated volume.
- When a public switch telephone line (PSTN) fax machine is not available and internet Protocols are used to fax, treat these systems as internet-connected systems, not as a fax machine using telephone protocols.

EMAIL

Email is a nearly ubiquitous communications medium and is widely used by election offices and voters. While this may be a convenient tool for distributing or receiving ballots, policy makers and election officials should be aware of the risks and challenges associated with email. Email provides limited security protections and is generally not considered suitable for sensitive communications. Email may be viewed or tampered with at multiple places in the transmission

process, and emails can also be forged to appear as if they were sent from a different address. Furthermore, email is often used in cyberattacks on organizations, such as attackers sending messages with malicious links or attachments to infect computers with malware. This malware could spread to other machines on the network if strong network segmentation techniques are not used.

- Use a dedicated computer that is separated from the remainder of the election infrastructure to receive and process these ballots. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.
- Patch and configure the computer—as well as document viewer software—against known vulnerabilities (e.g., disable active content, including JavaScript and macros.).
- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify U.S.-based government organizations on the internet.
- Use encryption where possible (e.g., implement STARTTLS on your email servers to create a secure connection, encrypt attached files, etc.)
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to help identify phishing emails.
- Implement DMARC, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on emails to help authenticate emails sent to voters.
- Utilize anti-malware detection and encourage voters to as well. Make sure to update the anti-malware regularly.
- Implement multi-factor authentication (MFA) on any email system used by election officials.
- Follow best practices for generating and protecting passwords and other authentication credentials.
- Use a dedicated, shared email address for receiving ballots, such as Ballots@County.Gov. Implement naming conventions in subject lines that will help identify emails as legitimate (e.g., 2020 Presidential General). While a dedicated, shared email account is typically not a best practice, in this instance, it segregates potentially malicious attachments from the network.

WEB-BASED PORTALS, FILE SERVERS, AND APPLICATIONS

Websites may provide accessible and user-friendly methods for transmitting ballots and other election data. While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks. Software vulnerabilities in web applications could allow attackers to modify, read, or delete sensitive information, or to gain access to other systems in the elections infrastructure. Sites that receive public input, such as web forms or uploaded files, may be particularly vulnerable to such attacks and should be used only after careful consideration of the risks, mitigations, and security/software engineering practices that went into that software.

- Avoid using knowledge-based authentication (e.g., address, driver's license number, social security number). To the extent practical, implement MFA for employees and voters and mandate MFA for all system administrators and other technical staff (including contractors).
- Patch and configure computers as well as document viewer software against known vulnerabilities (i.e., disable active content, including JavaScript and macros.).

- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify US-based government organizations on the internet.
- Use secure coding practices (e.g., sanitized inputs, parameter checking) for web applications.
- Encrypt traffic using Hypertext Transfer Protocol Secure (HTTPS) supporting Transport Layer Security (TLS) version 1.2. If you use a file server, ensure it uses a secure file transfer protocol, such as SFTP or FTPS.
- Ensure you have the bandwidth/capacity to handle the anticipated volume of traffic.
- Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.
- Develop a vulnerability management program (VMP). This allows well-meaning cybersecurity researchers to find and disclose vulnerabilities privately to an election official, giving the election official time to implement upgrades and patches before disclosing the information publicly.
- Place the application on a network that is continuously monitored, such as the network with a web application firewall, an Albert sensor, or an intrusion detection and prevention system.
- Carefully vet any third-party companies or contractors obtaining system access to perform security assessments or regular maintenance.
- Inform voters to only download the application from the trusted mobile application store.
- Encourage voters to use a trusted network and not an open Wi-Fi network.

RESOURCES

- CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at cisaservicedesk@cisa.dhs.gov.
- Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
- CISA's Binding Operational Directive (BOD)18-01 addresses enhancing email and web security.
- NIST Activities on UOCAVA Voting
- NIST special publication (SP) 800-177 provides recommendations and guidelines for enhancing trust in email.
- NIST SP 800-52r2 provides guidelines for selection, configuration, and use of TLS.
- FBI's Protected Voices initiative provides information and guidance on cybersecurity and foreign influence topics.
- The EAC's Election Security Preparedness webpage collects multiple resources that can assist election administrators.
- For more information about how election jurisdictions in the United States vote remotely, please see Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes.

APPENDIX: DETAILED RISK MAPPING

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
RISK: Exploitation of software flaws in election infrastructure			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	High
Web	High	High	High
RISK: Unauthorized modification(s) to blank ballots			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	N/A
Web	Low	Moderate	N/A
RISK: Loss of voted ballot integrity			
Fax	N/A	N/A	High
Email	N/A	N/A	High
Web	N/A	N/A	High
Risk: Loss of ballot secrecy			
Fax	N/A	N/A	Moderate
Email	N/A	N/A	High
Web	N/A	N/A	High
RISK: Unauthorized individual participates in voting channel			
Fax	Moderate	N/A	High
Email	Low	Low	High
Web	Low	Moderate	High

RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Risk: Broken Chain of Custody			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Low	Moderate	Moderate
RISK: Unable to access system or obtain ballot			
Fax	Low	N/A	Moderate
Email	Moderate	Moderate	High
Web	Moderate	High	High